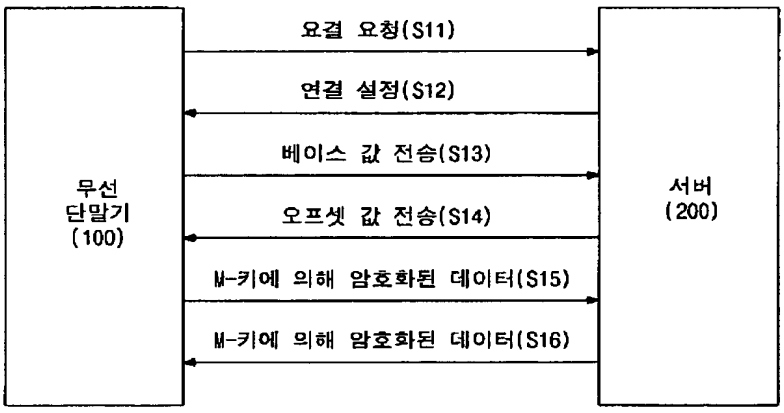
KOREAN PATENT ABSTRACTS(KR)

Document Code:A
(11) Publication No.1020020020166 (43) Publication.Date. 20020314
(21) Application No.1020010001265 (22) Application Date. 20010110
(51) IPC Code:
H04Q 7/38

(71) Applicant:
MQUAY INC.
(72) Inventor:
KWAK, U SEOP
(30) Priority:
1020000053062 20000907 KR

(54) Title of Invention
METHOD AND APPARATUS FOR CIPHERING/DECODING END-TO-END DATA IN WIRELESS DATA COMMUNICATION

Representative drawing



(57) Abstract:

PURPOSE: A method and an apparatus for ciphering/decoding end-to-end data in a wireless data communication are provided to shorten a ciphering/decoding time and embody a ciphering/decoding algorithm in a wireless terminal.

CONSTITUTION: A wireless terminal(100) requests connection to a server(200) (S11). The server(200) permits the connection request to the wireless terminal(100) and sets the connection(S12). The wireless terminal(100) transmits a base value necessary for generating a key used in a wireless data cipher/decoding to the server(200)(S13). The server (200) receives the base value and transmits an offset value necessary for generating the key to the wireless terminal(100)

(S14). All wireless data transmitted and received between the wireless terminal(100) and the server(200) are ciphered by the key to be transmitted(S15,S16), and an object decodes the received cipher sentence by the key and sees the data.

if display of image is failed, press (F5)

IPC-Code	H04Q 7/38				
Application No.	1020010001265	**Application Date**	20010110	**Doc Kind**	A
Unexamined Pub No.	1020020020166	**Unexamined Pub Date**	20020314		
Title of Invention	METHOD AND APPARATUS FOR CIPHERING/DECODING END-TO-END DATA IN WIRELESS DATA COMMUNICATION				
Priorty Country	KR	**Priorty No.**	1020000053062	**Priorty Date**	20000907

Applicant

Seq	Name
1	MQUAY INC.

Inventor

Seq	Name
1	KWAK, U SEOP

(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) Int. Cl.[7]
H04Q 7/38

(45) 공고일자 2003년05월16일
(11) 등록번호 10-0384183
(24) 등록일자 2003년05월02일

(21) 출원번호 10-2001-0001265
(22) 출원일자 2001년01월10일
(65) 공개번호 특2002-0020166
(43) 공개일자 2002년03월14일

(30) 우선권주장 1020000053062 2000년09월07일 대한민국(KR)
(73) 특허권자 주식회사 엠키
서울 강남구 포이동 219 동지빌딩 4층
(72) 발명자 곽우섭
경기도과천시중앙동30-5
(74) 대리인 이지연

심사관 : 민병준

(54) 무선 데이터 통신에서의 양단간 데이터 암호화/복호화방법 및 장치

요약

본 발명은 무선 데이터 통신에서 요구되는 양단간(end-to-end) 데이터 보안 방법에 관한 것으로서, 무선 단말기에서 서버로 연결 요청을 하는 단계와, 상기 무선 단말기의 연결 요청에 응답하여, 상기 서버가 상기 무선 단말기로 연결 설정을 하는 단계와, 상기 서버의 연결 설정에 응답하여, 상기 무선 단말기가 상기 서버로 베이스 값을 전송하는 단계와, 상기 전송된 베이스 값에 응답하여, 상기 서버가 상기 무선 단말기로 오프셋 값을 전송하는 단계와, 상기 서버 및 상기 무선 단말기가 각각 상기 베이스 값과 상기 오프셋 값을 기초로 암호화 키를 생성하는 단계와, 상기 서버 및 상기 무선 단말기는 각각 상기 암호화 키를 이용하여 데이터를 암호화하거나 복호화하는 단계를 포함한다.

본 발명에 의한 무선 데이터 통신을 위한 양단간 데이터 보안 방법은 종래의 암호화 방법들과는 달리 각각의 단말기가 개개의 고유한 키를 가지는 것이 아니라 무선 단말기가 서버에 접속할 때마다 새로운 키를 가지고 데이터를 암호화/복호화하기 때문에, 동일한 문장에 대해서도 항상 다르게 암호화가 되므로, 키가 노출되더라도 보안에 큰 문제가 없으며, 단말기 사용자 측면에서도 훨씬 더 보안성이 강화된 서비스를 받을 수 있게 된다.

대표도

도1

색인어

무선통신, 암호화, 복호화, 보안, 장치, 방법

명세서

도면의 간단한 설명

도1은 본 발명의 제1 실시예에 의한 무선 데이터 통신을 위한 양단간 데이터 보안 방법을 도시하는 흐름도.

도2는 본 발명의 제1 실시예에 의한 M-키를 생성하는 과정을 보여주는 개요도.

도3은 본 발명의 제1 실시예에 의한 M-키를 이용한 암호화/복호화 방법을 나타내는 개요도.

도4는 본 발명의 제2실시예에 의한 무선 단말기의 내부 구성을 도시하는 블록도.

도5은 본 발명의 제2 실시예에 의한 무선 데이터 통신을 위한 양단간 데이터 보안 방법을 도시하는 흐름도.

도6는 본 발명의 제2 실시예에 의한 M-키를 생성하는 과정을 보여주는 개요도.

도7는 본 발명의 제2 실시예에 의한 인증값이 서버에 저장되어 있는 모습을 보여주는 도표.

도8는 본 발명의 제3 실시예에 의한 무선 데이터 통신을 위한 양단간 데이터 보안 방법을 도시하는 흐름도.

도면의 주요 부분에 대한 부호의 설명

100: 무선 단말기 200: 서버

20: M-키 생성 함수

401: 무선 단말기의 인증값 저장 메모리

402: 최초 인증값 등록 모듈 403: 인증값 조회 모듈

404: 인증값 갱신 모듈

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 무선 데이터 통신에서 요구되는 양단간(end-to-end) 데이터 보안 방법에 관한 것으로서, 보다 구체적으로는 무선 데이터의 보안이 요구되는 은행, 증권사 등의 현금, 주식 등의 거래뿐만 아니라 개인 정보 보호에 필수적인 무선 데이터 양단간 암호화를 위하여, 현재의 단말기 및 서비스 서버의 환경에 효율적으로 적용할 수 있도록 적응된 무선 데이터 통신에서의 양단간 데이터 보안 방법에 관한 것이다.

유, 무선을 포함하여 양단간 데이터 보안 방법으로서 가장 일반적으로 사용되는 방법은 공개 키/비밀 키(public key/private key) 기반의 데이터 암호화 방법이다. 이 공개 키/비밀 키 기반의 데이터 암호화 방법은 하나의 키만을 사용하는 종래의 대칭 암호화 방법과는 대조적으로 두 개의 상이하지만 관련되어 있는 키를 사용하는 비대칭 암호화 방법이다.

공개 키/비밀 키 기반의 데이터 암호화 방법에 의한 데이터 보안은 다음과 같은 과정을 거쳐서 이루어진다.

a) 네트워크 상의 양단의 시스템이 한 쌍의 키(공개 키, 비밀 키)를 생성한다.

b) 각 시스템은 자신의 암호화 키를 공개 레지스터 또는 파일에 둠으로써 공개하고, 나머지 키는 비밀로 유지한다.

c) 만일 A 시스템이 B 시스템으로 메시지를 보내고자 한다면, B 시스템의 공개 키를 이용하여 메시지를 암호화한다.

d) B 시스템이 상기 메시지를 받으면, 자신의 비밀 키로 그 메시지를 복호화한다. B 시스템의 비밀 키는 B 시스템만이 알고 있으므로, 다른 수신 시스템은 A 시스템이 보낸 메시지를 해독하지 못한다.

이러한 공개 키/비밀 키 방식의 데이터 암호화 방법을 무선 데이터 통신에 적용할 경우에는 다음과 같은 문제점이 발생한다.

첫째, 계산 능력이 부족한 무선 단말기의 특성상 암호화 키가 긴 경우에는 데이터의 복호화가 제대로 되지 않는다는 문제점이 발생한다. 그 이유를 아래에서 설명한다.

상기 c, d 단계에서 이루어지는 암호화 및 복호화를 간략히 수식으로 표현하면 다음과 같다.

암호화 : 암호문(cipher Text) = $[\text{평문}]^{e} \pmod n$

복호화 : 평문(Plain Text) = $[\text{암호문}]^{d} \pmod n$

위의 수식에서 알 수 있는 바와 같이, 평문을 e제곱 연산하고, 이것을 n으로 나눈 나머지가 암호문이 되고, 암호문을 d제곱 연산하고 이것을 n으로 나눈 나머지가 원래의 평문이 된다. 그런데, 강력한 암호문을 만들기 위해서는 e,d 및 n이 큰 숫자이어야 하는데 그렇게 되면 많은 지수 연산을 하기 때문에 암호화/복호화를 위해서 많은 계산 능력이 필요하다. 특히, 학계의 발표에 의하면, 알고리즘의 특성상 복호화는 암호화에 비해 12배의 계산 능력이 필요하다.

따라서, 공개 키/비밀 키 방식의 데이터 암호화 방법을 무선 데이터 통신에 적용할 경우, 계산 능력이 부족한 무선 단말기의 특성상 암호화 키가 긴 경우에는 데이터의 복호화가 제대로 되지 않는다는 문제점이 발생하는 것이다. 실제로 현재 생산/판매되고 있는 무선 단말기에서 RSA 알고리즘을 적용하여 실험을 해 본 결과, 암호화 키가 8 바이트(64 비트)일 때, 암호화 속도가 크게 느려지지는 않았으나, 데이터를 복호화하는 도중에 무선 단말기가 다운되었다.

둘째, 공개 키/비밀 키 기반의 데이터 암호화 방법을 무선 데이터 통신에 적용할 경우, 단말기의 암호화 키가 노출된다면 단말기와 서버가 주고 받는 데이터의 보안이 보장되지 않는다는 문제점이 발생한다.

세째, 공개 키/비밀 키 방식의 데이터 암호화 방법은 동일한 평문에 대해서는 동일한 암호화문이 나오게 되므로, 암호화된 문장을 반복적으로 관찰한다면 암호화 키를 유추할 수 있다. 또한, 이동성이 장점인 단말기 내에 저장되어 있는 암호화 키가 복제될 수 있는 위험도 있다.

이와 같이, 공개 키/비밀 키 기반의 데이터 암호화 방법을 무선 데이터 통신에 적용할 경우 상기와 같은 문제점들이 발생하므로, 암호화/복호화가 제대로 이루어지고, 데이터의 보안이 보장되고, 단말기에 저장되어 있는 암호화 키의 복제에 대한 대비가 필요한, 보다 개선된 무선 데이터 통신에서의 암호화 알고리즘이 요구된다.

발명이 이루고자하는 기술적 과제

본 발명의 목적은 공개 키/비밀 키 방식의 데이터 암호화 방법을 무선 데이터 통신에 적용할 경우, 데이터의 복호화가 제대로 행해지지 않는 문제점 및 단말기의 암호화 키가 노출될 경우 무선 데이터의 보안이 보장되지 않는 문제점을 해결하는 것이다.

본 발명의 다른 목적은 암호화/복호화의 수치 계산의 과부하가 현저히 감소되는, 개선된 무선 데이터 통신에서의 양단간 보안 알고리즘을 제공하는 것이다.

본 발명의 다른 목적은 암호화 키의 유추와 단말기에 저장되어 있는 암호화 키의 복제에 대한 대비가 필요한, 개선된 무선 데이터 통신에서의 양단간 보안 알고리즘을 제공하는 것이다.

발명의 구성 및 작용

상기와 같은 목적을 달성하기 위하여, 본 발명의 제1 특징에 의한 무선 데이터 통신을 위한 양단간 데이터 보안 방법은 무선 단말기에서 서버로 연결 요청을 하는 단계와, 상기 무선 단말기의 연결 요청에 응답하여, 상기 서버가 상기 무선 단말기로 연결 설정을 하는 단계와, 상기 서버의 연결 설정에 응답하여, 상기 무선 단말기가 상기 서버로 베이스 값을 전송하는 단계와, 상기 전송된 베이스 값에 응답하여, 상기 서버가 상기 무선 단말기로 오프셋 값을 전송하는 단계와, 상기 서버 및 상기 무선 단말기가 각각 상기 베이스 값과 상기 오프셋 값을 기초로 암호화 키를 생성하는 단계와, 상기 서버 및 상기 무선 단말기는 각각 상기 암호화 키를 이용하여 데이터를 암호화하거나 복호화하는 단계를 포함하는 것을 특징으로 한다.

만일 서버가 베이스 값으로서 이미 암호화 키 생성에 필요한 단말기 정보를 가지고 있는 경우라면, 본 발명의 무선 데이터 통신을 위한 양단간 데이터 보안 방법은 무선 단말기에서 서버로 연결 요청을 하는 단계와, 상기 무선 단말기의 연결 요청에 응답하여, 상기 서버가 상기 무선 단말기로 연결 설정을 하는 단계와, 상기 서버가 상기 무선 단말기로 오프셋 값을 전송하는 단계와, 상기 서버 및 상기 무선 단말기가 각각 상기 단말기 정보와 상기 오프셋 값을 기초로 암호화 키를 생성하는 단계와, 상기 서버 및 상기 무선 단말기는 각각 상기 암호화 키를 이용하여 데이터를 암호화하거나 복호화하는 단계를 포함하는 것을 특징으로 한다.

또한, 본 발명의 제2 특징에 의한 무선 데이터 통신을 위한 양단간 데이터 보안 방법은 무선 단말기에서 서버로 연결 요청을 하는 단계와, 상기 무선 단말기의 연결 요청에 응답하여, 상기 서버가 상기 무선 단말기로 연결 설정을 하는 단계와, 상기 서버의 연결 설정에 응답하여, 상기 무선 단말기가 상기 서버로 베이스 값을 전송하는 단계와, 상기 전송된 베이스 값에 응답하여, 상기 서버가 상기 무선 단말기로 오프셋 값과 인증값 갱신 플래그를 전송하는 단계와, 상기 서버 및 상기 무선 단말기가 각각 상기 베이스 값, 상기 오프셋 값, 및 상기 무선 단말기가 저장하고 있는 인증값을 기초로 암호화 키를 생성하는 단계와, 상기 서버 및 상기 무선 단말기는 각각 상기 암호화 키를 이용하여 데이터를 암호화하거나 복호화하는 단계를 포함하는 것을 특징으로 한다.

만일 상기 인증값 갱신 플래그의 값이 인증값 갱신을 지시하는 경우라면, 상기 무선 단말기가 상기 인증값을 갱신하는 단계를 더 포함하는데, 상기 인증값 갱신 단계는 (a) 상기 무선 단말기가 상기 서버로 새로운 인증값을 요청하는 단계와, (b) 상기 요청에 응답하여 상기 서버가 상기 무선 단말기로 인증값을 전송하는 단계와, (c) 상기 무선 단말기가 상기 전송된 인증값을 상기 서버로 전송하는 단계와, (d) 상기 서버가 상기 무선 단말기로 전송한 인증값과 상기 무선 단말기로부터 수신한 인증값이 동일하다고 판단하는 경우, 갱신 완료 메시지를 상기 무선 단말기로 전송하고, 상이하다고 판단하는 경우, 갱신 실패 메시지를 상기 무선 단말기로 전송하는 단계와, 상기 무선 단말기가 상기 서버로부터 갱신 실패 메시지를 수신한 경우, 상기 서버로부터 갱신 완료 메시지를 수신할 때까지 (a)~(d)의 단계를 소정의 횟수만큼 반복하는 단계를 포함하는 것을 특징으로 한다.

또한, 본 발명의 제3 특징에 의한 무선 데이터 통신을 위한 양단간 데이터 보안 방법은 무선 단말기에서 서버로 연결 요청을 하는 단계와, 상기 무선 단말기의 연결 요청에 응답하여, 상기 서버가 상기 무선 단말기로 연결 설정을 하는 단계와, 상기 서버의 연결 설정에 응답하여, 상기 무선 단말기가 베이스 값, 오프셋 값, 및 인증값을 기초로 암호화 키를 생성하는 단계와, 상기 무선 단말기가 상기 베이스 값, 상기 오프셋 값, 및 상기 암호화 키를 이용하여 암호화한 요청 업무를 상기 서버로 전송하는 단계와, 상기 서버가 상기 무선 단말기로부터 전송된 상기 베이스 값 및 상기 오프셋 값, 및 상기 서버가 관리하는 상기 무선 단말기의 인증값을 기초로 암호화 키를 생성하는 단계와, 상기 서버가 상기 암호화 키를 이용하여 상기 전송된 요청 업무를 복호화하여 처리하고, 상기 처리 결과, 인증값 갱신 플래그, 및 새로운 인증값을 상기 무선 단말기로 전송하는 단계를 포함하는 것을 특징으로 한다.

만일 상기 인증값 갱신 플래그의 값이 인증값 갱신을 지시하는 경우라면, 본 발명의 제3 특징에 의한 무선 데이터 통신을 위한 양단간 데이터 보안 방법은 상기 무선 단말기는 상기 새로운 인증값으로 인증값을 갱신하는 단계를 더 포함한다.

본 발명에 의한 무선 데이터 통신을 위한 양단간 데이터 보안 방법은 종래의 암호화 방법들과는 달리 각

각의 단말기가 개개의 고유한 키를 가지는 것이 아니라 무선 단말기가 서버에 접속할 때마다 새로운 키를 가지고 데이터를 암호화/복호화하는 것을 특징으로 한다.

이렇게 함으로써 동일한 문장에 대해서도 항상 다르게 암호화가 되므로, 키가 노출되더라도 보안에 큰 문제가 없으며, 단말기 사용자 측면에서도 훨씬 더 보안성이 강화된 서비스를 받을 수 있게 된다.

이하, 첨부된 도면에 의해 본 발명의 바람직한 실시예들을 상세히 설명하기로 한다.

실시예1

실시예1에서는 무선 단말기가 서버에 접속할 때마다, 베이스 값을 서버로 전송하고, 서버는 무선 단말기로 오프셋 값을 전송하며, 서버와 무선 단말기는 각각 이러한 베이스 값과 오프셋 값을 기초로 암호화 키를 생성한다. 만일 서버가 이미 베이스 값을 가지고 있는 경우라면, 무선 단말기가 서버로 베이스 값을 전송할 필요 없이, 서버만 무선 단말기로 오프셋 값을 전송한 후, 서버와 무선 단말기는 각각 이러한 베이스 값과 오프셋 값을 기초로 암호화 키를 생성한다.

도1은 본 발명의 제1 실시예에 의한 무선 데이터 통신을 위한 양단간 데이터 보안 방법을 도시하는 흐름도이다. 도1에 도시된 바와 같이, 우선 무선 단말기(100)가 서버(200)로 연결 요청을 한다(S11). 연결 요청을 받은 서버(200)는 무선 단말기(100)에 연결 요청을 허가하고 연결 설정을 한다(S12). 무선 단말기(100)는 본 발명에 의한 무선 데이터 암호화/복호화에 사용되는 키(이하, M-키라 한다)의 생성에 필요한 베이스 값을 서버로 전송한다(S13). 서버(200)는 베이스 값을 수신하고, M-키 생성에 필요한 오프셋 값을 무선 단말기(100)로 전송한다(S14). 여기서, 무선 단말기(100)가 서버(200)로 보내는 베이스 값은 전화 번호 또는 기기 번호(ESN, electronic serial number), 또는 난수와 같은 단말기 생성 정보이고, 서버(200)가 무선 단말기(100)로 보내는 오프셋 값은 날짜, 시간, PID(process ID), 또는 액세스 순서와 같은 랜덤 수일 수 있다.

무선 단말기(100)와 서버(200)가 이와 같이 베이스 값과 오프셋 값을 주고 받고 나면, 무선 단말기(100)와 서버(200)는 각자 베이스 값과 오프셋 값을 가지고 M-키를 생성한다. 이 M-키 생성 원리는 도2에 도시되어 있다.

도2에 도시된 바와 같이, M-키(23)는 베이스 값(21)으로부터 추출한 값과 오프셋 값(22)으로부터 추출한 값, 이 두 가지 값을 입력 값으로 하여 단방향 해쉬 함수(one-way hash function, 20)를 통해서 만들게 된다. 여기서, 단방향 해쉬 함수는 역함수가 존재하지 않는 해쉬 함수(non-inverted hash function)로서 결과 값인 키를 가지고 유추될 수는 없다. 단방향 해쉬 함수를 수식으로 나타내면 다음과 같다.

f(베이스 값, 오프셋 값) = M-키, f^{-1}는 존재하지 않음

단방향 해쉬 함수 대신에, 본 발명의 다른 실시예로서 DES에서 사용되는 비선형 부울 함수, 또는 베이스 값과 오프셋 값을 입력 값으로 하는 난수 발생 함수가 사용될 수도 있으나, 이들 함수 역시 역함수가 존재하지 않아야 한다. 왜냐하면, 암호문을 분석하여 암호화 키를 알아내었을 경우에 암호화 키를 만든 함수의 역함수가 존재한다면 암호화 키를 만드는 알고리듬을 유추할 수 있기 때문이다.

도2에 도시된 원리에 의해 M-키가 생성된 이후에, 도1에 도시된 바와 같이, 무선 단말기(100)와 서버(200)간에 오가는 모든 무선 데이터는 M-키로 암호화되어서 보내어지고(S15, S16), 상대편에서는 수신된 암호문을 M-키로 해독하여 데이터를 보게 된다. 이로써, 무선 데이터 통신에서의 양단간 데이터 보안이 이루어지게 된다.

M-키를 이용하여 데이터를 암호화하거나 복호화하는 방법에 대해서는 이하에서 도3을 참조하여 구체적으로 설명한다.

우선, M-키를 이용한 암호화 방법에 대해서 살펴보면, M-키를 이용한 암호화 방법은 전체 데이터(평문)를 일정한 크기의 여러 블록으로 나누어서 각각의 데이터 블록을 암호화하고, 암호화된 각각의 블록을 하나로 합치는 과정으로 이루어져 있다. 즉, 본 발명에 의한 M-키를 이용한 암호화 방법은 도3에 도시된 바와 같이, 전체 데이터(평문)를 블록 단위로 자르는 단계(S31), M-키를 이용하여 각각의 블록을 암호화하는 단계(S32), 및 암호화된 블록을 합치는 단계(S33)를 포함한다. 이러한 암호화 과정에 사용되는 알고리듬은 블록 암호화(block cipher) 알고리듬으로서, 일반적으로 사용되고 있는 알고리듬이다. 블록 암호화 알고리듬 대신에, 본 발명의 다른 실시예로서 스트림 암호화(stream cipher) 알고리듬이 사용될 수도 있다.

한편, M-키를 이용한 복호화 방법은 암호화 방법과 반대되는 것으로서, 전체 데이터(암호문)를 일정한 크기의 여러 블록으로 나누어서 각 데이터 블록을 복호화하고, 복호화된 각각의 블록을 하나로 합치는 과정으로 이루어져 있다. 즉, 본 발명에 의한 M-키를 이용한 복호화 방법은 도3에 도시된 바와 같이, 전체 데이터(암호문)를 일정 크기의 블록 단위로 자르는 단계(S34), M-키를 이용하여 각각의 블록을 복호화하는 단계(S35), 및 복호화된 블록을 합치는 단계(S36)를 포함한다.

여기서, 암호화/복호화에 걸리는 시간을 살펴보면, 종래의 공개 키/비밀 키 방식의 데이터 암호화 방법에서는 암호화/복호화를 위하여 우선 키 검색이 필요하기 때문에 이진 검색(binary search) 알고리듬에 의해 최소한 $O(\log n)$(n은 키의 갯수)의 타임 컴플렉시티(time complexity)가 걸리나, 본 발명의 M-키를 이용한 암호화/복호화 방법에서는 M-키가 1회성 암호화/복호화 키이므로, 키 검색 시간이 별도로 들지 않고 키 생성 시간만 필요하다. 따라서, 본 발명은 $O(1)$의 타임 컴플렉시티가 걸린다.

또한, 종래의 공개 키/비밀 키 방식의 데이터 암호화 방법은 전술한 바와 같이 비대칭 암호화 방법으로서 알고리듬의 특성상 복호화 시간이 암호화 시간에 비해 12배 정도 들지만, 본 발명의 M-키에 의한 데

이터 암호화 방법은 대칭 암호화 방법이므로 복호화 시간이 암호화 시간과 동일하다.

이와 같이, 본 발명의 M-키를 이용한 암호화/복호화 방법은 종래의 공개 키/비밀 키 방식의 데이터 암호화 방법에 비해 암호화/복호화 시간이 훨씬 단축될 뿐만 아니라, 암호화/복호화 알고리듬이 복잡하지 않으므로 계산 능력이 부족한 무선 단말기에도 충분히 구현할 수 있다. 실제로 본 발명에 따라 16 바이트(128 비트) 암호화 키를 이용하여 SEED 암호화 알고리즘을 적용하여 실험해 본 결과, 무선 단말기에 무리 없이 암호화/복호화가 잘 이루어졌다.

또한, 서버 접속 시마다 새로운 키를 생성하므로, 만약 M-키가 노출되었다 하더라도 노출된 M-키는 1회용이고 다음 연결 설정 시에는 다른 M-키를 사용하기 때문에 안전한 보안 통신 상태를 유지할 수 있으며, 키가 노출된 경우 종래의 방법에서는 새로운 키를 단말기에 저장해야 하나, 본 발명의 방법에서는 이러한 번거로움이 없다.

또한, 동일한 평문에 대한 암호문이 항상 다르게 되므로, 암호문을 통한 암호화 키의 유추로 인한 키 유출을 방지할 수도 있다.

특히, 본 발명의 제1 실시예에 의하면, 서버가 모든 가입자의 공개 키 및 서버의 비밀 키를 보관하기 위한 키 관리 서버를 별도로 운영할 필요가 없고, 최초에 각각의 단말기로 공개 키와 비밀 키를 분배할 필요도 없기 때문에, 데이터 암호화/복호화에 많은 자원을 낭비하지 않게 됨으로써, 매우 효율적으로 전체 서버 시스템의 자원을 사용할 수 있고, 이에 따라 똑같은 서버에서 보다 많은 사용자에게 통신 보안을 제공할 수 있다. 단말기의 입장에서도 자신의 비밀 키와 서버의 공개 키를 저장하기 위한 별도의 저장 공간을 가지고 있을 필요가 없다.

이하에서는, 도1에 도시된 것과 같은, 본 발명의 제1 실시예에 의한 양단간 데이터 보안 방법이 어떻게 구현되는지에 대해 더욱 구체적으로 설명하기 위해, 4 바이트 암호화 키를 예로 들어 설명한다.

우선, 무선 단말기는 M-키 생성에 필요한 베이스 값으로서 자신의 전화 번호인 01x-234-5678을 서버로 전송한다. 서버는 무선 단말기로부터 베이스 값을 수신한 후, M-키 생성에 필요한 오프셋 값으로서 현재 시각인 20000901141234를 무선 단말기로 전송한다.

무선 단말기는 자신이 서버로 전송한 베이스 값(01x-234-5678)과 서버로부터 받은 오프셋 값(20000901142322)을 입력 값으로 하여 단방향 해쉬 함수를 통해 M-키를 생성하는데, 예를 들면, 베이스 값(01x-234-5678)의 맨 뒤 4자리인 5678과 오프셋 값(20000901142322)의 맨 뒤 4자리인 1234를 더한 다음 이 더한 값 6912를 단방향 해쉬 함수의 입력으로 하여 M-키인 6173을 만든다. 한편, 서버도 무선 단말기로부터 받은 베이스 값(01x-234-5678)과 무선 단말기로 전송한 오프셋 값(20000901142322)을 이용하여 무선 단말기에서와 같이 M-키인 6173을 만든다.

서버와 무선 단말기 모두가 암호화를 위한 동일한 M-키를 가지고 있으므로, 전송하고자 하는 평문은 M-키를 가지고 암호화한 다음 전송하고, 수신한 암호문은 M-키를 가지고 평문으로 해독하여 볼 수 있다. 예를 들면, 평문을 4 바이트 단위로 자른 다음에 M-키인 6173을 이용하여 4 바이트 단위로 암호화 연산을 한 다음 이를 결합하면 암호문이 되고, 이 암호문을 4 바이트 단위로 자른 다음에 M-키인 6173을 이용하여 4 바이트 단위로 복호화 연산을 한 다음 이를 결합하면 평문이 된다.

지금까지는 서버와 무선 단말기가 서로 베이스 값과 오프셋 값을 주고 받아서 M-키를 생성하는 경우를 설명하였지만, 서버가 이미 베이스 값으로서 단말기 정보를 가지고 있는 경우라면, 무선 단말기에서 서버로 베이스 값을 전송할 필요가 없이 서버에서 무선 단말기로만 오프셋 값을 전송한 다음, 무선 단말기와 서버에서 각각 단말기 정보(베이스 값)와 오프셋 값을 이용하여 M-키를 생성할 수 있다.

실시예2

실시예2에서도 실시예1에서와 마찬가지로 무선 단말기가 서버에 접속할 ??마다 베이스 값과 오프셋 값을 주고 받는다. 그러나, 실시예2에서는 M-키를 만들 때, 베이스 값과 오프셋 값뿐만 아니라, 무선 단말기 내부에 저장된 인증값(authentification value)도 이용한다. 또한, 이러한 인증값은 서버의 지시에 따라 일정 시기 경과 후에 갱신될 수 있다. 여기서, 인증값이란 통신에 필요한 암호화 키를 만드는데 사용되는 파라미터로서, 무선 단말기내에 암호화되어 저장되어 있는 값이다.

먼저 도4을 참조하여, 본 발명의 제2 실시예에 따른 무선 단말기(100) 내부의 구성을 설명한다.

무선 단말기(100) 내에는 도4에 도시된 바와 같이, 인증값이 저장되어 있는 메모리(401)와, 이 인증값을 처리하는 3개의 모듈, 즉, 최초 인증값 등록 모듈(402), 인증값 조회 모듈(403), 및 인증값 갱신 모듈(404)이 존재한다.

최초 인증값 등록 모듈(402)은 무선 단말기(100)가 생성된 이후 최초의 통신을 위해 필요한 암호화 키를 만드는데 필요한 인증값을 무선 단말기 메모리(401)에 등록하는 모듈로서, 서비스 제공 기관에서 제공하는 인증값을 단말기의 고유정보를 파라미터로 하는 암호화 키에 의해 암호화하여 단말기의 특정 영역(401)에 저장한다. 단말기에 최초로 인증값을 입력하는 방법으로는, 단말기의 자판을 통해 입력하는 방식과 단말기에 직렬 케이블을 연결하여 전송하는 방식이 있다.

인증값 조회 모듈(403)은 암호화 키를 만들기 위한 파라미터로서 인증값이 요청될 ??, 단말기 메모리(401)에 암호화되어 저장되어 있는 인증값을 복호화한 후, 전달한다.

인증값 갱신 모듈(404)은 인증값 갱신 요청이 있을 때 단말기 메모리의 인증값을 갱신한다.

도5는 본 발명의 제2 실시예에 의한 무선 데이터 통신을 위한 양단간 데이터 보안 방법을 도시하는 흐름도이다. 도5에 도시된 바와 같이, 우선 무선 단말기(100)가 서버(200)로 연결 요청을 한다(S51). 연결 요청을 받은 서버(200)는 무선 단말기(100)에 연결 요청을 허가하고 연결 설정을 한다(S52). 무선 단말기(100)는 M-키의 생성에 필요한 베이스 값을 서버(200)로 전송한다(S53). 서버(200)는 베이스 값을 수신하고, M-키 생성에 필요한 오프셋 값과 인증값 갱신 플래그를 무선 단말기(100)로 전송한다(S54). 여기서, 인증값 갱신 플래그란 무선 단말기가 가지고 있는 인증값을 갱신해야 하느냐 여부를 나타내는 값으로서, 참일 때는 " 갱신해야 한다" , 거짓일 때는 " 갱신할 필요가 없다" 라는 것을 나타낸다. 이러한 인증값 갱신 플래그의 결정은 서비스 제공 기관의 정책에 달려있다. 현재 유선 인터넷 상에서 인증값의 갱신 주기는 통상 6개월 정도가 된다.

이러한 전송 단계 완료 후에, 무선 단말기(100)와 서버(200)는 각자 베이스 값, 오프셋 값,인증값을 가지고 M-키를 생성한다. 이 M-키 생성 원리는 도6에 도시되어 있다.

도6에 도시된 바와 같이, M-키(64)는 베이스 값(61)으로부터 추출한 값, 오프셋 값(62)으로부터 추출한 값, 그리고, 인증값(63), 이 3가지 값을 입력 값으로 하여 단방향 해쉬 함수(one-way hash function, 60)를 통해서 만들게 된다. 단방향 해쉬 함수에 관해서는 실시예1에서 설명하였으므로 여기서 이에 대한 설명은 생략한다.

도6에 도시된 원리에 의해 M-키가 생성된 이후에, 무선 단말기(100)와 서버(200)간에 오가는 모든 무선 데이터는 M-키로 암호화되어서 보내어지고, 상대편에서는 수신된 암호문을 M-키로 해독하여 데이터를 보게 된다. 이로써, 무선 데이터 통신에서의 양단간 데이터 보안이 이루어지게 된다.

이하에서는, 인증값의 갱신에 대해 설명한다.

도5에서 단계(S56~S59)는 인증값 갱신이 일어나는 경우에만 해당되는 단계이다.

전술한 바와 같이, 서버(200)와 무선 단말기(100)가 각자 베이스 값, 오프셋 값, 인증값을 가지고 M-키를 생성한 이후, 무선 단말기(100)는 서버(200)가 보내준 인증값 갱신 플래그의 값을 체크한다.

만일 인증값 갱신 플래그의 값이 참이라면, 인증값을 갱신해야 한다는 것을 나타내므로,무선 단말기(100)는 서버(200)에게 새로운 인증값을 보내줄 것을 요청한다(S56). 이에 응답하여, 서버(200)는 무선 단말기(100)로 새로운 인증값을 보내준다(S57). 무선 단말기(100)는 서버(200)로부터 인증값을 제대로 받았는지 확인하기 위하여, 서버(200)로부터 받은 상기 인증값을 다시 서버(200)로 전송한다(S58). 서버(200)는 자신이 무선 단말기(100)로 보낸 인증값과 무선 단말기(100)가 자신에게 보내준 인증값을 비교하여 그 값이 동일하면, 무선 단말기가 인증값을 제대로 수신하였다는 메시지를 전송한다(S59). 이로써, 인증값 갱신이 완료되며, 갱신된 인증값은 다음 번의 서버와 무선 단말기간의 접속 때부터 M-키를 생성하는데 사용된다.

만일 서버(200)가 무선 단말기(100)로 보낸 인증값과 무선 단말기(100)가 서버(200)로 보내준 인증값이 상이하다면, 무선 단말기(100)가 서버(200)로부터 인증값을 제대로 받지 못한 것이므로, 도5의 절차(S56 ~ S59)를 소정의 횟수만큼(예: 3회) 반복한다. 만일 소정의 횟수만큼 도5의 절차(S56 ~ S59)를 반복했는데도 무선 단말기(100)가 인증값을 제대로 받지 못하면, 더 이상의 시도는 하지 않고, 문제가 있다는 메시지를 전송한다.

여기서, 인증값을 갱신하기 위해 무선 단말기(100)와 서버(200)간에 이루어지는 모든 절차(S56 ~ S59)는 당연히 M-키에 의해 암호화된 상태에서 이루어진다.

한편, 무선 단말기(100)가 서버(200)로부터 수신한 인증값 갱신 플래그의 값이 거짓인 경우에는, 무선 단말기(100)가 현재 가지고 있는 인증값을 갱신할 필요가 없으므로, 현재의 인증값을 그대로 사용한다.

도7은 서버(200)가 각 무선 단말기(100)의 인증값을 관리하는 모습을 나타내는 데이터 구조이다.

도7에 도시된 바와 같이, 서버에는 각 무선 단말기에 대해서 서버(200)가 무선 단말기(100)로부터 수신한 베이스 값(701), 인증값(702), 및 갱신 날짜(703)가 저장되어 있으며, 서버(200)는 베이스 값(701)을 기준으로 하여 해당 무선 단말기의 인증값(702)을 찾아낼 수 있다.

또한, 서버는 인증값이 갱신된 날짜(703)와 현재의 날짜를 비교하여 일정 주기로 인증값을 갱신해주게 된다.

본 발명의 제2 실시예에 의하면, 제1 실시예에서와 마찬가지로, 종래의 공개 키/비밀 키 방식의 데이터 암호화 방법에 비해 암호화/복호화 시간이 훨씬 단축될 뿐만 아니라, 암호화/복호화 알고리듬이 복잡하지 않으므로 계산 능력이 부족한 무선 단말기에도 충분히 구현할 수 있고, 서버 접속 시마다 새로운 키를 생성하므로, 만약 M-키가 노출되었다 하더라도 안전한 보안 상태를 유지할 수 있으며, 동일한 평문에 대한 암호문이 항상 다르게 되므로 암호문을 통한 암호화 키의 유추로 인한 키 유출을 방지할 수도 있다.

특히, 본 발명의 제2 실시예에 의하면, 베이스 값과 오프셋 값 뿐만 아니라, 서비스 제공 기관에서 관리하는 인증값을 파라미터로 하여 M 키를 생성하기 때문에, 보안 알고리듬 제공 회사가 인증값을 알 수 없으므로, 네트워크상에 공개된 베이스 값과 오프셋 값만 가지고 암호화 키를 만드는 제1 실시예에 비해, 더욱 완벽하게 보안이 보장되는 효과가 있다.

또한, 단말기 내에 저장되어 있는 인증값도 그대로 저장되는 것이 아니라 단말기마다 상이한 암호화 키

에 의해 암호화되어 저장되기 때문에 인증값 복제에 대한 방지를 할 수 있다.

이하에서는, 도5에 도시된 것과 같은, 본 발명의 실시예2에 따른 양단간 데이터 보안 방법이 어떻게 구현되는지에 대해 더욱 구체적으로 설명하기 위해, 4 바이트 암호화 키를 예로 들어 설명한다.

우선, 무선 단말기는 M-키 생성에 필요한 베이스 값으로서 자신의 전화 번호인 01x-234-5678을 서버로 전송한다. 서버는 무선 단말기로부터 베이스 값을 수신한 후, M-키 생성에 필요한 오프셋 값으로서 현재 시각인 20000901141234와 인증값 갱신 플래그를 무선 단말기로 전송한다.

무선 단말기는 자신이 서버로 전송한 베이스 값(01x-234-5678)과 서버로부터 받은 오프셋 값(20000901142322), 그리고 인증값(1017)을 입력 값으로 하여 단방향 해쉬 함수를 통해 M-키를 생성하는데, 예를 들면, 베이스 값(01x-234-5678)의 맨 뒤 4자리인 5678과 오프셋 값(20000901142322)의 맨 뒤 4자리인 1234, 그리고 인증값 1017을 더한 다음, 이 더한 값 7929를 단방향 해쉬 함수의 입력으로 하여 M-키인 6173을 만든다. 한편, 서버도 무선 단말기로부터 받은 베이스 값(01x-234-5678)과 무선 단말기로 전송한 오프셋 값(20000901142322), 그리고 서버에 저장되어 있는 사용자의 인증값(1017)을 이용하여 무선 단말기에서와 같이 M-키인 6173을 만든다.

서버와 무선 단말기 모두가 암호화를 위한 동일한 M-키를 가지고 있으므로, 전송하고자 하는 평문은 M-키를 가지고 암호화한 다음 전송하고, 수신한 암호문은 M-키를 가지고 평문으로 해독하여 볼 수 있다. 예를 들면, 평문을 4 바이트 단위로 자른 다음에 M-키인 6173을 이용하여 4 바이트 단위로 암호화 연산을 한 다음 이를 결합하면 암호문이 되고, 이 암호문을 4 바이트 단위로 자른 다음에 M-키인 6173을 이용하여 4 바이트 단위로 복호화 연산을 한 다음 이를 결합하면 평문이 된다.

만약 무선 단말기가 서버로부터 받은 인증값 갱신 플래그가 참인 경우에는 무선 단말기는 서버에 대해 새로운 인증값을 요구하고, 서버는 무선 단말기로 새로운 인증값(2137)을 보낸다. 무선 단말기는 서버로부터 받은 인증값을 서버로 다시 보내 인증값의 확인을 요청하며, 서버는 자신이 무선 단말기로 보낸 인증값과 무선 단말기가 자신에게 보내준 인증값을 비교하여 그 값이 동일하면, 무선 단말기가 인증값을 제대로 수신하였다는 메시지를 전송한다. 이로써, 인증값 갱신이 완료되며, 인증값으로서 이전의 값 1017 대신에 2137이 저장된다. 갱신된 새로운 인증값(2137)은 다음번 접속할 때 사용된다.만일 서버가 무선 단말기로 보낸 인증값과 무선 단말기가 서버로 다시 보낸 인증값이 상이하면, 무선 단말기가 인증값을 제대로 수신하지 못한 것이므로, 인증값 갱신을 위한 절차를 소정의 회수만큼 반복한다. 만일 이러한 추가적인 절차에 의해서도 무선 단말기가 인증값을 제대로 수신하지 못하면, 인증값 갱신은 취소되고 보안 관리자에게 알려지게 된다.

실시예3

실시예3은 실시예2에서의 절차를 좀더 간소화한 것으로서, 무선 단말기와 서버가 데이터를 주고 받는 통신 절차를 줄이고 싶은 경우에 사용될 수 있는 방법이다.

도8은 본 발명의 제3 실시예에 의한 무선 데이터 통신을 위한 양단간 데이터 보안 방법을 도시하는 흐름도이다. 도8에 도시된 바와 같이, 우선 무선 단말기(100)가 서버(200)로 연결 요청을 한다(S81). 연결 요청을 받은 서버(200)는 무선 단말기(100)에 연결 요청을 허가하고 연결 설정을 한다(S82). 무선 단말기(100)는 베이스 값, 오프셋 값, 및 인증값을 가지고 M-키를 생성한다(S83). 무선 단말기(100)는 서버(200)로 베이스 값과 오프셋 값을 포함하는 평문 및 M-키로 암호화된 사용자 요청 업무를 포함하는 복합문(평문+암호문)을 전송한다(S84). 여기서, 암호화된 사용자 요청 업무를 신용카드 결제로 예를 들면, 카드 결제에 필요한 정보, 즉, 카드 번호, 유효 기간, 승인 금액 등이 될 수 있다.

서버(200)는 무선 단말기(100)가 보내준 평문 속의 베이스 값, 오프셋 값, 및 서버(200)에서 보관하고 있는 해당 사용자의 인증값을 가지고 M-키를 생성한다(S85). 서버(200)는 무선 단말기(100)가 보낸 사용자 요청 업무를 M-키를 가지고 복호화 하여 해당 업무를 처리한 다음, 사용자 요청 업무의 결과값과 인증값 갱신에 필요한 제어값을 M-키로 암호화 해서 전송한다(S86). 제어값에는 인증값 갱신 플래그, 새로운 인증값 등이 포함되어 있어서, 인증값 갱신 플래그가 참인 경우에는 함께 전송된 새로운 인증값으로 인증값을 갱신하는 절차를 밟으며, 인증값 갱신 플래그가 거짓인 경우에는 함께 전송된 값을 무시하게 된다.

본 발명은 무선 단말기를 통해서 조회, 이체와 같은 은행 업무를 처리하고자 할 때, 고객의 단말기와 은행 계정계/정보계 서버 사이의 계좌번호, 각종 비밀번호 등의 무선 데이터의 보안에 적용될 수 있고, 무선 단말기를 통해 주가 조회, 매수/매도 주문과 같은 증권 업무를 처리하고자 할 때, 고객의 단말기와 증권사 서버 사이의 증권 계좌번호, 매수/매도 주문 정보, 각종 비밀번호 등의 무선 데이터 보안에 적용될 수 있으며, 수배자 조회, 도난차량 검색과 같은 경찰의 실시간 업무를 처리할 때, 차량 정보나 개인의 신상 정보 등의 데이터 보안에 적용될 수 있으며, 무선 단말기를 통해 상품의 주문/결제와 같은 무선 전자 상거래를 하고자 할 때, 개인의 신상정보, 카드번호, 계좌번호 및 각종 비밀번호 등의 무선 데이터 보안에 적용될 수 있다.

또한, 본 발명의 양단간 데이터 보안 방법이 주로 무선 데이터 통신을 위한 것이나, 연산 능력(computing power)이 부족하거나 메모리가 작은 경우의 유선 데이터 통신 환경에서도 사용될 수 있다.

이상 본 발명을 실시예를 사용하여 설명하였지만, 본 발명의 범위는 특정 실시예에 한정되는 것은 아니며, 첨부된 특허청구범위에 의해서 해석되어야 할 것이다.

발명의 효과

본 발명에 의하면, 종래의 공개 키/비밀 키 방식의 데이터 암호화 방법에 비해 암호화/복호화 시간이 훨씬 단축될 뿐만 아니라, 암호화/복호화 알고리듬이 복잡하지 않으므로 계산 능력이 부족한 무선 단말기에도 충분히 구현할 수 있으며, 단말기가 서버에 접속할 때마다 새로운 암호화 키를 만들기 때문에 동일한 문장에 대해서도 항상 다르게 암호화가 되므로, 키가 노출되더라도 보안에 큰 문제가 없다.

특히, 본 발명의 제1 실시예에 의하면, 서버가 모든 가입자의 공개키 및 서버의 비밀키를 보관하기 위한 키 관리 서버를 별도로 운영할 필요가 없으므로, 데이터 암호화/복호화에 많은 자원을 낭비하지 않게 됨으로써, 매우 효율적으로 전체 서버 시스템의 자원을 사용할 수 있다.

또한, 본 발명의 제2 실시예에 의하면, 베이스 값과 오프셋 값 뿐만 아니라, 서비스 제공 기관에서 관리하는 인증값을 파라미터로 하여 M 키를 생성하기 때문에, 보안 알고리듬 제공 회사가 인증값을 알 수 없으므로, 네트워크상에 공개된 베이스 값과 오프셋 값만 가지고 암호화 키를 만드는 제1 실시예에 비해, 더욱 완벽하게 보안이 보장되는 효과가 있고, 단말기 내에 암호화되어 저장되어 있는 인증값을 일정 주기로 갱신함으로써, 보다 강력한 보안성을 제공할 수 있다.

따라서, 본 발명에 의한 무선 데이터 통신에서의 양단간 암호화 방법은 현재의 무선 단말기의 하드웨어 및 소프트웨어 환경에서 가장 효율적인 암호화 방법이 될 수 있다.

(57) 청구의 범위

청구항 1

무선 데이터 통신을 위한 양단간 데이터 보안 방법에 있어서,

무선 단말기에서 서버로 연결 요청을 하는 단계;

상기 무선 단말기의 연결 요청에 응답하여, 상기 서버가 상기 무선 단말기로 연결 설정을 하는 단계;

상기 서버의 연결 설정에 응답하여, 상기 무선 단말기가 상기 서버로 베이스 값을 전송하는 단계;

상기 전송된 베이스 값에 응답하여, 상기 서버가 상기 무선 단말기로 오프셋 값을 전송하는 단계;

상기 서버 및 상기 무선 단말기가 각각 상기 베이스 값과 상기 오프셋 값을 기초로 암호화 키를 생성하는 단계; 및

상기 서버 및 상기 무선 단말기는 각각 상기 암호화 키를 이용하여 데이터를 암호화하거나 복호화하는 단계를 포함하는 무선 데이터 통신을 위한 양단간 데이터 보안 방법.

청구항 2

무선 데이터 통신을 위한 양단간 데이터 보안 방법으로서, 서버가 암호화 키 생성에 필요한 단말기 정보를 베이스 값으로서 가지고 있는 양단간 데이터 보안 방법에 있어서,

무선 단말기에서 서버로 연결 요청을 하는 단계;

상기 무선 단말기의 연결 요청에 응답하여, 상기 서버가 상기 무선 단말기로 연결 설정을 하는 단계;

상기 서버가 상기 무선 단말기로 오프셋 값을 전송하는 단계;

상기 서버 및 상기 무선 단말기가 각각 상기 단말기 정보와 상기 오프셋 값을 기초로 암호화 키를 생성하는 단계; 및

상기 서버 및 상기 무선 단말기는 각각 상기 암호화 키를 이용하여 데이터를 암호화하거나 복호화하는 단계를 포함하는 무선 데이터 통신을 위한 양단간 데이터 보안 방법.

청구항 3

무선 데이터 통신을 위한 양단간 데이터 보안 방법에 있어서,

무선 단말기에서 서버로 연결 요청을 하는 단계;

상기 무선 단말기의 연결 요청에 응답하여, 상기 서버가 상기 무선 단말기로 연결 설정을 하는 단계;

상기 서버의 연결 설정에 응답하여, 상기 무선 단말기가 상기 서버로 베이스 값을 전송하는 단계;

상기 전송된 베이스 값에 응답하여, 상기 서버가 상기 무선 단말기로 오프셋 값과 인증값 갱신 플래그를 전송하는 단계;

상기 서버 및 상기 무선 단말기가 각각 상기 베이스 값, 상기 오프셋 값, 및 상기 무선 단말기가 저장하고 있는 인증값을 기초로 암호화 키를 생성하는 단계; 및

상기 서버 및 상기 무선 단말기는 각각 상기 암호화 키를 이용하여 데이터를 암호화하거나 복호화하는 단계를 포함하는 무선 데이터 통신을 위한 양단간 데이터 보안 방법.

청구항 4

제3항에 있어서, 상기 인증값 갱신 플래그의 값이 인증값 갱신을 지시하는 경우, 상기 무선 단말기가 상기 인증값을 갱신하는 단계를 더 포함하는 무선 데이터 통신을 위한 양단간 데이터 보안 방법.

청구항 5

제4항에 있어서, 상기 인증값 갱신 단계는

(a) 상기 무선 단말기가 상기 서버로 새로운 인증값을 요청하는 단계;

(b) 상기 요청에 응답하여 상기 서버가 상기 무선 단말기로 인증값을 전송하는 단계;

(c) 상기 무선 단말기가 상기 전송된 인증값을 상기 서버로 전송하는 단계;

(d) 상기 서버가 상기 무선 단말기로 전송한 인증값과 상기 무선 단말기로부터 수신한 인증값이 동일하다고 판단하는 경우, 갱신 완료 메시지를 상기 무선 단말기로 전송하고, 상이하다고 판단하는 경우, 갱신 실패 메시지를 상기 무선 단말기로 전송하는 단계; 및

(e) 상기 무선 단말기가 상기 서버로부터 갱신 실패 메시지를 수신한 경우, 상기 서버로부터 갱신 완료 메시지를 수신할 때까지 (a)~(d)의 단계를 소정의 횟수만큼 반복하는 단계를 포함하는 무선 데이터 통신을 위한 양단간 데이터 보안 방법.

청구항 6

무선 데이터 통신을 위한 양단간 데이터 보안 방법에 있어서,

무선 단말기에서 서버로 연결 요청을 하는 단계;

상기 무선 단말기의 연결 요청에 응답하여, 상기 서버가 상기 무선 단말기로 연결 설정을 하는 단계;

상기 서버의 연결 설정에 응답하여, 상기 무선 단말기가 베이스 값, 오프셋 값, 및 인증값을 기초로 암호화 키를 생성하는 단계;

상기 무선 단말기가 상기 베이스 값, 상기 오프셋 값, 및 상기 암호화 키를 이용하여 암호화한 요청 업무를 상기 서버로 전송하는 단계;

상기 서버가 상기 무선 단말기로부터 전송된 상기 베이스 값 및 상기 오프셋 값, 및 상기 서버가 관리하는 상기 무선 단말기의 인증값을 기초로 암호화 키를 생성하는 단계; 및

상기 서버가 상기 암호화 키를 이용하여 상기 전송된 요청 업무를 복호화하여 처리하고, 상기 처리 결과, 인증값 갱신 플래그, 및 새로운 인증값을 상기 무선 단말기로 전송하는 단계를 포함하는 무선 데이터 통신을 위한 양단간 데이터 보안 방법.

청구항 7

제6항에 있어서, 상기 인증값 갱신 플래그의 값이 인증값 갱신을 지시하는 경우, 상기 무선 단말기는 상기 새로운 인증값으로 인증값을 갱신하는 단계를 더 포함하는 무선 데이터 통신을 위한 양단간 데이터 보안 방법.

청구항 8

제1항 내지 제7항 중 어느 한 항에 있어서, 상기 암호화 키는 단방향 해쉬 함수(one-way hash function), DES에서 사용되는 비선형 부울 함수, 또는 난수 발생 함수에 의해 생성되는 무선 데이터 통신을 위한 양단간 데이터 보안 방법.

청구항 9

제1항 내지 제7항 중 어느 한 항에 있어서, 상기 암호화 키를 이용한 암호화 단계는

평문(plain text)을 일정 크기의 데이터 블록으로 나누는 단계;

상기 나뉘어진 데이터 블록을 상기 암호화 키를 이용하여 각각 암호화하는 단계; 및

상기 암호화된 각 블록을 결합하는 단계를 포함하는 무선 데이터 통신을 위한 양단간 데이터 보안 방법.

청구항 10

제1항 또는 제7항 중 어느 한 항에 있어서, 상기 암호화 키를 이용한 복호화 단계는

암호문(cipher text)을 일정 크기의 데이터 블록으로 나누는 단계;

상기 나뉘어진 데이터 블록을 상기 암호화 키를 이용하여 각각 복호화하는 단계; 및

상기 복호화된 각 블록을 결합하는 단계를 포함하는 무선 데이터 통신을 위한 양단간 데이터 보안 방법.

청구항 11

제1항 내지 제7항 중 어느 한 항에 있어서, 상기 베이스 값은 전화 번호 또는 기기 번호(ESN, electronic serial number) 또는 난수를 포함하는 단말기 생성 정보인 무선 데이터 통신을 위한 양단간 데이터 보안 방법.

청구항 12

제1항 내지 제7항 중 어느 한 항에 있어서, 상기 오프셋 값은 날짜, 시간, PID(process ID), 또는 액세스 순서를 포함하는 랜덤 수인 무선 데이터 통신을 위한 양단간 데이터 보안 방법.

청구항 13

무선 데이터 통신을 위한 양단간 데이터 보안 장치에 있어서,

무선 단말기로부터 연결 요청을 받는 수단;

상기 무선 단말기의 연결 요청에 응답하여, 상기 무선 단말기로 연결 설정을 하는 수단;

상기 무선 단말기로부터 베이스 값을 수신하는 수단;

상기 수신한 베이스 값에 응답하여, 상기 무선 단말기로 오프셋 값을 전송하는 수단;

상기 베이스 값과 상기 오프셋 값을 기초로 암호화 키를 생성하는 수단;

상기 암호화 키를 이용하여 데이터를 암호화하는 수단; 및

상기 암호화 키를 이용하여 암호화된 데이터를, 상기 무선 단말기로부터 수신하여 복호화하는 수단을 포함하는 무선 데이터 통신을 위한 양단간 데이터 보안 장치.

청구항 14

무선 데이터 통신을 위한 양단간 데이터 보안 장치로서, 암호화 키 생성에 필요한 단말기 정보를 베이스 값으로서 가지고 있는 양단간 데이터 보안 장치에 있어서,

무선 단말기로부터 연결 요청을 받는 수단;

상기 무선 단말기의 연결 요청에 응답하여, 상기 무선 단말기로 연결 설정을 하는 수단;

상기 무선 단말기로 오프셋 값을 전송하는 수단;

상기 단말기 정보와 상기 오프셋 값을 기초로 암호화 키를 생성하는 수단;

상기 암호화 키를 이용하여 데이터를 암호화하는 수단; 및

상기 암호화 키를 이용하여 암호화된 데이터를, 상기 무선 단말기로부터 수신하여 복호화하는 수단을 포함하는 데이터 통신을 위한 양단간 데이터 보안 장치.

청구항 15

삭제

청구항 16

삭제

청구항 17

삭제

청구항 18

유선 데이터 통신을 위한 양단간 데이터 보안 방법에 있어서,

단말기에서 서버로 연결 요청을 하는 단계;

상기 단말기의 연결 요청에 응답하여, 상기 서버가 상기 단말기로 연결 설정을 하는 단계;

상기 서버의 연결 설정에 응답하여, 상기 단말기가 상기 서버로 베이스 값을 전송하는 단계;

상기 전송된 베이스 값에 응답하여, 상기 서버가 상기 단말기로 오프셋 값을 전송하는 단계;

상기 서버 및 상기 단말기가 각각 상기 베이스 값과 상기 오프셋 값을 기초로 암호화 키를 생성하는 단계; 및

상기 서버 및 상기 단말기는 각각 상기 암호화 키를 이용하여 데이터를 암호화하거나 복호화하는 단계를 포함하는 유선 데이터 통신을 위한 양단간 데이터 보안 방법.

청구항 19

유선 데이터 통신을 위한 양단간 데이터 보안 방법으로서, 서버가 암호화 키 생성에 필요한 단말기 정보를 베이스 값으로서 가지고 있는 양단간 데이터 보안 방법에 있어서,

단말기에서 서버로 연결 요청을 하는 단계;

상기 단말기의 연결 요청에 응답하여, 상기 서버가 상기 단말기로 연결 설정을 하는 단계;

상기 서버가 상기 단말기로 오프셋 값을 전송하는 단계;

상기 서버 및 상기 단말기가 각각 상기 단말기 정보와 상기 오프셋 값을 기초로 암호화 키를 생성하는 단계; 및

상기 서버 및 상기 단말기는 각각 상기 암호화 키를 이용하여 데이터를 암호화하거나 복호화하는 단계를 포함하는 유선 데이터 통신을 위한 양단간 데이터 보안 방법.

청구항 20

유선 데이터 통신을 위한 양단간 데이터 보안 방법에 있어서,

단말기에서 서버로 연결 요청을 하는 단계;

상기 단말기의 연결 요청에 응답하여, 상기 서버가 상기 단말기로 연결 설정을 하는 단계;

상기 서버의 연결 설정에 응답하여, 상기 단말기가 상기 서버로 베이스 값을 전송하는 단계;

상기 전송된 베이스 값에 응답하여, 상기 서버가 상기 단말기로 오프셋 값과 인증값 갱신 플래그를 전송하는 단계;

상기 서버 및 상기 단말기가 각각 상기 베이스 값, 상기 오프셋 값, 및 상기 단말기가 저장하고 있는 인증값을 기초로 암호화 키를 생성하는 단계; 및

상기 서버 및 상기 단말기는 각각 상기 암호화 키를 이용하여 데이터를 암호화하거나 복호화하는 단계를 포함하는 유선 데이터 통신을 위한 양단간 데이터 보안 방법.

청구항 21

유선 데이터 통신을 위한 양단간 데이터 보안 방법에 있어서,

단말기에서 서버로 연결 요청을 하는 단계;

상기 단말기의 연결 요청에 응답하여, 상기 서버가 상기 단말기로 연결 설정을 하는 단계;

상기 서버의 연결 설정에 응답하여, 상기 단말기가 베이스 값, 오프셋 값, 및 인증값을 기초로 암호화 키를 생성하는 단계;

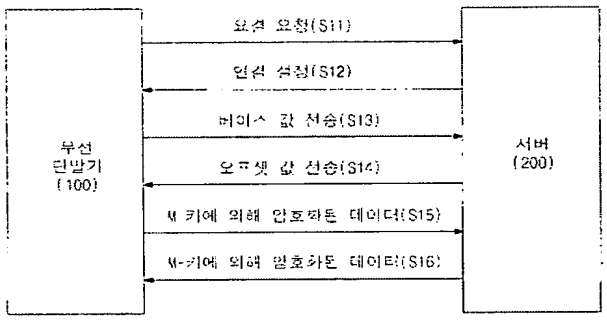
상기 단말기가 상기 베이스 값, 상기 오프셋 값, 및 상기 암호화 키를 이용하여 암호화한 요청 업무를 상기 서버로 전송하는 단계;

상기 서버가 상기 단말기로부터 전송된 상기 베이스 값 및 상기 오프셋 값, 및 상기 서버가 관리하는 상기 단말기의 인증값을 기초로 암호화 키를 생성하는 단계; 및

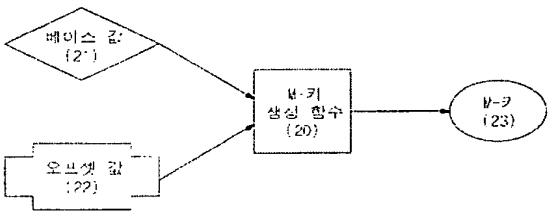
상기 서버가 상기 암호화 키를 이용하여 상기 전송된 요청 업무를 복호화하여 처리하고, 상기 처리 결과, 인증값 갱신 플래그, 및 새로운 인증값을 상기 단말기로 전송하는 단계를 포함하는 유선 데이터 통신을 위한 양단간 데이터 보안 방법.

도면

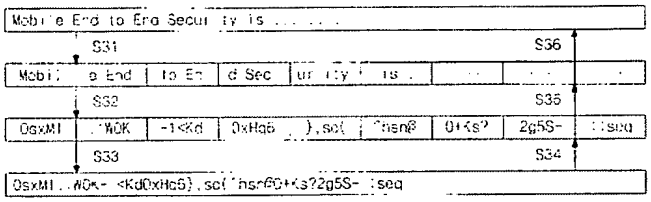
도면1



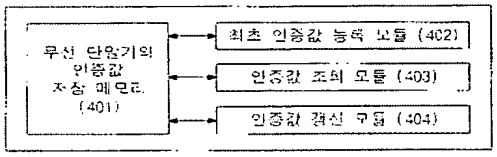
도면2



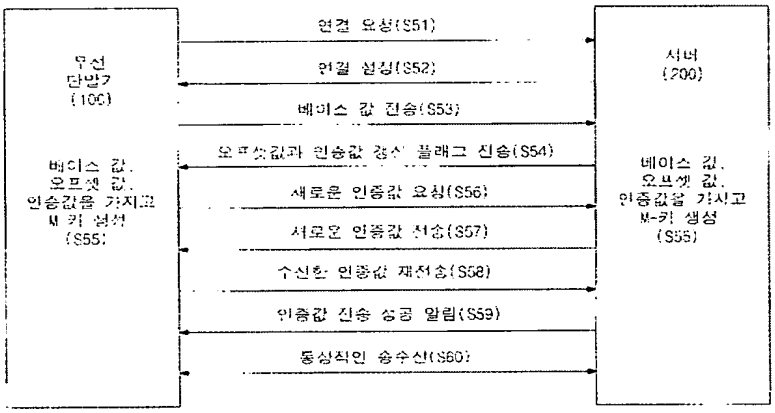
도면3



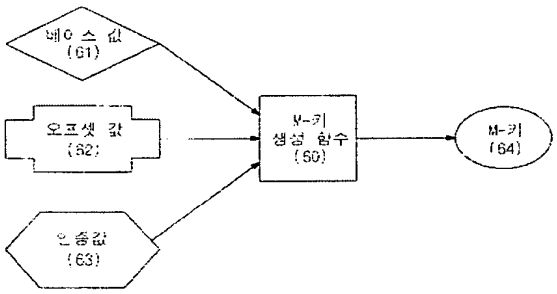
도면4



도면5



도면6



도면7

베이스 값 (701)	인증값(16바이트) (702)	갱신 날짜 (703)
0192345555	0x1234567890AAAAAA	2000/12/02
0192346666	0x1234567890BBB33B	2000/12/11
0192347777	0x1234567890CCCCCC	2000/11/28
0192348888	0x1234567890DDDDDD	2000/12/09

도면8